

Poznámky z Kombinatorických štruktúr

Peter Csiba, petherz@gmail.com, <https://github.com/Petrzlen/fmfi-poznamky>

17.01.2013

Obsah

1	Úvod	3
2	Latinské štvorce	3
2.1	Metrika medzi permutáciami	3
2.1.1	Vseobecna metrika	3
2.1.2	Metricky system permutácii	3
2.2	Hallova veta	3
2.3	Normalizovane LS	4
2.4	Ortogonalne LS	4
2.5	Polonormalizovane LS	4
2.6	Uplna mnozina.	4
3	Vyvazene blokové plány	4
3.1	Vlastnosti	5
3.2	Bruck, Ryser	5
3.3	Diferencne množiny	5
3.3.1	Definované na \mathbb{Z}_v	5
3.3.2	Definované na grupach	5
4	Hadamardove matice	6
4.1	Vlastnosti	6
4.2	Konstrukcie	6
4.2.1	Sylvestrova	6
4.2.2	Kroneckerov súčin	6
4.3	Hadamardova hypotéza	6
4.4	Ekvivalencia s blokovými plánmi	7
5	Konečné projektívne roviny	7
5.1	Desarguesova veta	7
5.2	Vlastnosti	7
5.3	(v, k, λ) -konfigurácie	7
5.4	Existencia projektívnej roviny	8
5.5	Ortonormalné latinské štvorce	8
5.5.1	LS a PR	8
5.6	Singerove diferenciálne množiny	8

6	Nevyvážené blokové plány	8
6.1	Vlastnosti	9
7	Steinerovské systémy trojic	9
7.1	Věta Kirkman	9
7.2	Konstrukce	9
7.2.1	Projektivní SST	9
7.2.2	Afinní SST	9
7.2.3	Přímý sudý SST	10
7.2.4	$2n + 1$ konstrukce	10
7.2.5	Wilsonova-Schreiberova konstrukce	10
7.3	Částečný SST	10
7.4	T-design	10
7.4.1	Steinerovské systémy stvořit	10
7.4.2	Steinerovské systémy petič	10
7.5	Projektivní speciální lineární grupy	10
7.5.1	Mathieuovy grupy	10
8	Symetrické konfigurace	11
8.1	Například	11
9	Matroidy	11
9.1	Definice	11
9.2	Speciální matroidy	11
9.3	Vlastnosti	12
9.4	Hodnotová funkce	12

1 Úvod

Autor neabsolvoval prednášky ani skúšku z predmetu Kombinatorické štruktúry. Poznámky sú voľným prepisom poznámok Martina Šrámečka doplnených o komentár autora.

Nakoniec poznamenajme, že autor sa snažil písať pravdu a len pravdu, keďže jeho odpoveď na skúškach vychádza z tototo materiálu. Ak čitateľ chce prispieť ku kvalite textu, nech autorovi napíše a ten mu udelí prístup do repozitára.

2 Latinské štvorce

- $n \times n$
- $\{1, \dots, n\} = X$
- Každý riadok aj stĺpec je permutácia.
- S_n sym. grupa $n!$
- Φ, Ψ - permutacie na X
- Φ, Ψ su *dis...ntne* na Y ak $\forall x \in Y \Psi(x) \neq \Phi(x)$
- Φ, Ψ su *dis...ntne* \Leftrightarrow su *dis...ntne* na X

Poznámky.

- Latinsky stvorec - maximalny latinsky obdlznik.
- Maximalna mnoznina navzajom maximalne vzdialenych permutacii.

2.1 Metrika medzi permutaciami

2.1.1 Vseobecna metrika

- $S(x, y) = 0 \Leftrightarrow x = y$
- $S(x, y) = S(y, x)$
- $S(x, y) + S(y, z) \geq S(x, z)$

1

2.1.2 Metricky system permutacii

- $S(\Psi, \Phi)$ - max pocet prvkov mnoziny $Y \subseteq X$ pri ktorej Ψ a Φ su *dis...ntne*.
- $S(\Psi, \Phi) = |\{x \in X, \Psi(x) \neq \Phi(x)\}|$
- $S(\Psi, \Phi) = S(\Phi^{-1}\Psi, id)$

2.2 Hallova veta

Latinsky stvorec je maximalna mnozina *dis...permutacii* z S_n . $L_n = [\Phi_1, \dots, \Phi_n]$.

¹ Podla pravidla o generalizacii kde nedavame kvantifikatory, tak su vseobecne.

Hallova veta. Nech (X_1, \dots, X_k) je system množin $X_i \subseteq X$. $T \subseteq X$ je system rozlicnych reprezentantov ak $T = [x_1, \dots, x_k], x_i \in X_i, x_i \neq x_j$ pre $i \neq j$. Potom system X ma system rozlicnych reprezentantov \Leftrightarrow pre kazdy system množin $Y \subseteq X$ plati $|\cup Y_i| \geq |Y|$.

Veta. Kazdy latinsky obdlznik sa da doplnit na stvorec. Lebo Hallova veta.

2.3 Normalizovane LS

1 2 ...
2
3
...

2.4 Ortogonalne LS

- $L_n = [\Phi_1, \dots, \Phi_n]$ jeden LS
- $L'_n = [\Phi_1, \dots, \Phi_n]$ sruhy LS
- $L_n \perp L'_n \Leftrightarrow (i, j) \neq (k, l) \in X \times X$ plati $(\Phi_i(j), \Phi'_i(j)) \neq (\Phi_k(l), \Phi'_k(l))$
- Tj. vsetky dvojice (i, j) .

Vlastnosti 1-2.

- $L_n \perp L'_n \Leftrightarrow L_n \cdot L'_n$ je LS.
- Ak $L_n \perp L'_n \Rightarrow \forall \Phi, \Psi \in S_n : \Psi L_n \perp \Phi L'_n \wedge L_n \Psi \perp L'_n \Phi$.

2.5 Polonormalizovane LS

$[id, \Phi_2, \dots, \Phi_n]$.

Vlastnost 3. Nech $L_n^{(1)}, \dots, L_n^{(r)}$ je množina navzajom \perp LS. Potom $r \leq n-1$. TODO - polonormalizovane prelozene cez seba.

2.6 Uplna množina.

Uplna množina. Uplna množina $L_n^{(1)}, \dots, L_n^{(n-1)}$ je množina $n-1$ LS.

Sievers. Nech $n = p^r$, kde p je prvočíslo a $n \geq 1$. Potom existuje uplna množina $(n-1)$ navzajom ortogonalnych LS radu n . TODO - $\exists GF(n) = F$, technicky sporom.

3 Vyvazene blokové plány

(v, k, λ) -konfigurácia.

- $X = \{x_1, \dots, x_v\}$ - body.
- System podmnožin $B = X_1, \dots, X_n$ - bloky.
- 1. $|X_i| = k$ (konst)

- 2. $X_i \cap X_j = \lambda$ (konst) $i \neq j$.
- 3. $0 < \lambda < k < v - 1$

Incidenčna matica. $A = (a_{ij}), a_{ij} = 1 \Leftrightarrow x_j \in X_i$

Jednotková matica. $J = (1)$

3.1 Vlastnosti

1. $AJ = kJ$
2. $AA^T = \lambda J + (k - \lambda)I$
3. $\det(AA^T) = (\det A)^2 = [k + \lambda(v - 1)](k - \lambda)^{v-1} > 0$, TODO, rozvoj podľa riadka
4. $k(k - 1) = \lambda(v - 1)$, TODO, z AA^T na JAJ .
5. $JA = AJ = kJ$, TODO
6. $AA^T = A^T A$, zameniteľnosť blokov a bodov, TODO

3.2 Bruck, Ryser

Nutné podmienky na existenciu (v, k, λ) konfigurácie:

- v je párne, tak $k - \lambda$ je stvorec
- v je nepárne, $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \lambda yz$ má nenulové riešenie v \mathbb{Z} .

3.3 Diferencné množiny

Špeciálny prípad.

3.3.1 Definované na \mathbb{Z}_v

$\mathbb{Z}_v \supseteq D = \{d_1, \dots, d_k\}$, ak každý prvok $a \in \mathbb{Z}_v - 0$ sa dá vyjadriť λ rôznymi spôsobmi ako rozdiel dvoch prvkov z D .

Konstrukcia.

- $X = \mathbb{Z}_v$
- $X_i = D + i$

Napríklad $X = \mathbb{Z}_7, D = \{1, 2, 4\}$ dáva $[1, 2, 4], [2, 3, 5], [3, 4, 6], [4, 5, 0], [5, 6, 1], [6, 0, 2], [0, 1, 3]$ - Fannova rovina $(7, 3, 1)$.

3.3.2 Definované na grupách

Nech G je konečná grupa radu v , nie nutne komutatívna. Množina $D = \{d_1, \dots, d_k\} \subseteq G$ sa nazýva DM založená na G , ak je splnená jedna z dvoch podmienok:

- $\forall a \neq e \exists \lambda (d_i, d_j), i \neq j : a = d_i d_j^{-1}$
- $\forall a \neq e \exists \lambda (d_i, d_j), i \neq j : a = d_i^{-1} d_j$

Tvrdenie. Každá (v, k, λ) dif. množina založená na G definuje (v, k, λ) konfiguráciu:

- $X = G$
- $B = \{Dg, g \in G\}$

TODO

Příklad. $(16, 6, 2)$ -konfigurácia.

- $G = \mathbb{Z}_4$
- $D = \{(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1), (1, 1, 0, 0), (0, 0, 1, 1)\}$

4 Hadamardove matice

Len stručne. Nechcelo sa mi texovať matice. $H_n = (a_{ij})$

- (i) $a_{ij} = \pm 1$
- (ii) $HH^T = nI$ - navzájom ortogonálne, maximálny objem spomedzi jednotkových

4.1 Vlastnosti

Základné.

1. $\langle H_i, H_j \rangle = n$ ak $i = j$, 0 ak $i \neq j$. Len iný zápis (ii)
2. H je uzavretá na výmenu riadkov a stĺpcov, násobenie -1
3. Každá H je normálna, tj. $HH^T = H^T H$.
4. Každú H maticu je možné previesť na normálnu - prvý riadok a prvý stĺpec má samé 1.

Deliteľnosť 4. $n = 1$ or $n = 2$ or $4 | n$. Normalizácia. Spočítame koľko je typov stĺpcov podľa prvých torč riadkov.

4.2 Konštrukcie

4.2.1 Sylvestrova

$$\begin{array}{cc} H & H \\ H & -H \end{array}$$

4.2.2 Kroneckerov súčin

$$\begin{array}{ccc} a_{11}H & \dots & a_{1n}H \\ \dots & \dots & \dots \\ a_{n1}H & \dots & a_{nn}H \end{array}$$

4.3 Hadamardova hypotéza

Pre každé n deliteľné 4 existuje matica. Neznáme su pre 168,224,284,312. (Najdi bug).

4.4 Ekvivalencia s blokovými planmi

Normalizované H matice sú ekvivalentné s $(4n - 1, 2n - 1, n - 1)$ -konfiguráciami. TODO: Triválne.

Kvadraticke rezidua. TODO. Kvadraticke rezidua $-i$. Diferenčná množina $-i$. Hadamardova matica.

5 Konečné projektívne roviny

Uz len to najdôležitejšie.

- $V_{n+1}(F) = F^{n+1} - 0$
- (PP1) Každými dvoma bodmi vedie práve jedna priamka.
- (PP2) Každé dve priamky majú práve jeden spoločný bod.
- (PP3) Existujú štyri rôzne body vo všeobecnej polohe (žiadne tri z nich nie sú kolineárne)

Priklady.

- Polgula kde stotožníme priamky cez s bodmi na obale.
- $\mathbb{Z}_2^3 - 0$
- Znížením dimenzie. Stotožníme body $y = kx, k \in F$.

5.1 Desarguesova veta

Ak sú trojuholníky T_1, T_2 perspektívne z bodu S , tak sú perspektívne aj z priamky.

5.2 Vlastnosti

Nech $n \geq 2$, Π je projektívna geometria. NPSE:

1. Nejaka priamka obsahuje práve $n + 1$ bodov.
2. Nejakým bodom prechádza práve $n + 1$ priamok.
3. Každá priamka obsahuje presne $n + 1$ bodov.
4. Každým bodom prechádza $n + 1$ priamok.
5. V Π sa nachádza presne $n^2 + n + 1$ bodov.
6. V Π sa nachádza presne $n^2 + n + 1$ priamok.

Oznacenie. n -rad projektívnej roviny

5.3 (v, k, λ) -konfigurácie

Každá projektívna rovina, ktorá má na nejakej priamke konečný počet bodov definuje (v, k, λ) -konfiguráciu:

- $v = n^2 + n + 1$ - body
- $k = n + 1$ - priamka obsahujúca body
- $\lambda = 1$ - priesečníky priamok

5.4 Existencia projektívnej roviny

Tvrdenie. Pre existenciu proj. roviny radu n je nutné, aby pre $n \equiv 1, 2 \pmod{4}$ existovali a, b , take, že $n = a^2 + b^2$. Bez dokazu.

Hypoteza. PR radu n existuje iba pre $n = p^r$.

5.5 Ortonormalne latinske stvorce

Latinska vlastnost. Matica $C = (c_{ij})$ rozmerov $n \times (t+2)$ ma *latinsku vlastnost*, ak $(c_{ik}, c_{il}) \neq (c_{jk}, c_{jl})$.

Lema. Nech $n \geq 3$ a $t \geq 2$ su z \mathbb{N} . Potom mnozina t navzajom roznych ortogonalnych latinskych stvorcov radu n existuje \Leftrightarrow existuje matica $C = (c_{ij})$, $n \times (t+2)$ s latinskou vlastnostou. TODO. Ake su rozmery matice v dokaze?

Veta. Ak existuje mnozina t navzajom ortogonalnych LS radu n a mnozina t ortogonalnych LS radu m , tak existuje aj mnozina t OLS radu nm .

Dosledok. $n = p^{\alpha_1} \dots p^{\alpha_k}$.

5.5.1 LS a PR

Veta. Nech $n \geq 3$. Potom PR radu n existuje \Leftrightarrow existuje $n-1$ navzajom ortogonalnych LS radu n .

\Rightarrow . Fixujeme jednu priamku $X = x_1, \dots, x_{n+1}$. Zvysnych n^2 bodov oznacime y_1, \dots, y_{n^2} . Priamky prechadzajuce x_j oznacime postupne L_{j1}, \dots, L_{jn} . Potom $c_{ij} = k \Leftrightarrow y_i \in L_{jk}$. Sporom. \Leftarrow . Majme $n-1$ OLS radu n a skonstruujeme C rozmerov $n^2 \times (n+1)$ s LV. Bod a hodnota v C urcuju na ktorej priamke lezi $y_i \in L_{jk}$. TODO.

5.6 Singerove diferencne mnoziny

PG. Kvadraticke rezidua. Bikvadraticke rezidua. Tetrakvadraticke rezidua.

6 Nevyvazene blokové plány

Nevyvazena (b, r, v, k, λ) -konfiguracia je system podmnozín-blokov $\{X_1, \dots, X_b\}$, $X_i \subseteq X$, kde $X = \{x_1, \dots, x_v\}$ a plati:

1. $|X_i| = k$
2. x_i sa vyskytuje prave v r blokoch
3. x_i, x_j sa spolocne vyskytuju v λ blokoch
4. $0 < \lambda, k < v-1$ (netrivialnost)

Steinerovske systemy trojic. $k=3, \lambda=1$.

Graf K_v^λ . Kompletny graf o v vrchoch s λ nasobnymi hranami. (b, r, v, k, λ) -konfiguracia odpovedaju jej rozkladu.

6.1 Vlastnosti

Incidenčná matica $b \times v$.

1. $AJ_v = kJ_{b,v}$
2. $J_bA = rJ_{b,v}$
3. $AA^T = \lambda J_v - (r - \lambda)I_v$
4. $bk = vr$. Zratame dvojice dvoma roznyimi sposobmi.
5. $r(k - 1) = \lambda(v - 1)$. Zratame dvojice s fixnym prvkom.
6. $\det(A^T A) = (r + \lambda(v - 1))(r - \lambda)^{v-1}$
7. $b \geq v$ (Fischerova nerovnosť). Dokaz z predoslych dvoch. Dosledok $r \geq k$.

7 Steinerovske systémy trojíc

SST je dvojica $S = (P, B)$ kde

- $|P| = v$
- B ke systém trojprvkových podmnožín P takých, že $\forall \{x_i, x_j\} \in \frac{P}{2}$ patri práve do jednej trojice.

Zjavne blokovo plan je $k = 3$ a $\lambda = 1$. Mozeme nahliadnuť na SST ako na rozklad K_v na K_3 .

7.1 Veta Kirkman

Tvrdenie. Nutne $v \equiv 1, 3 \pmod{6}$

Veta. Pre každé $v \equiv 1, 3 \pmod{6}$ existuje SST. $N(v) \geq (e^{-5}v)^{\frac{v^2}{6}}$. Bez dokazu.

7.2 Konštrukcie

7.2.1 Projektívne SST

- $\mathbb{Z}_2^{n+1} - 0$ - body $PG(2, n)$
- bloky $\{x, y, z\}$, $x + y + z = 0$ - priamky v $PG(2, n)$

TODO

7.2.2 Afinne SST

- \mathbb{Z}_3^n - body $AG(3, n)$
- bloky $\{x, y, z\}$ - priamky v $PG(2, n)$

TODO

7.2.3 Priamy sucin SST

- $R = (P, B)$
- $S = (Q, C)$
- $R \times S = (P \times Q, D)$

D obsahuje bloky v jednom z troch tvarov. TODO

7.2.4 $2n + 1$ konstrukcia

TODO

7.2.5 Wilsonova-Schreiberova konstrukcia

- Abelovska grupa A radu n .
- $P = A \cup \{\alpha, \beta\}$
- TODO
- TODO

7.3 Ciastocny SST

Pozadujeme, aby kazda dvojica bodov bola nanajvys v jednej trojici.

Tvrdenie. Kazdy SST sa da (s pridaním nejakého počtu bodov) doplniť na SST. TODO: niekde chyba ciastocny.

7.4 T-design

Steinerovsky system $S(t, k, n)$ je t -blokovy plan, taky, ze $\lambda = 1$. (System k -prvkovych podmnozín n -prvkovej množiny taky, ze kazda t -prvkova podmnozina je obsiahnuta v prave jednom bloku.) Navyse musi platit $1 < t < k < n$.

7.4.1 Steinerovske systemy stvoric

$S(3, 4, n)$

7.4.2 Steinerovske systemy petic

$S(4, 5, n)$

7.5 Projektivne specialne linearne grupy

k -tranzitivita, ostrá k -tranzitivita. TODO.

Tvrdenie (Klasifikacia $K \cup G$). TODO

7.5.1 Mathieuove grupy

TODO

8 Symetricke konfiguracie

- Kazdym bodom prechadza k priamok (kazdy bod je v k blokoch)
- Kazda priamka prechadza k bodmi (velkost bloku je k)

8.1 Napriklad

- 7_3 - Fannova rovina
- 8_3 - Mobius-Kantor
- 9_3 - Pappus z Alexandrie
- 10_3 - Desargues
- 15_3 - Cremona-Richmond

TODO

9 Matroidy

Axiomatizacia linearnej nezávislosti.

9.1 Definicia

- X - konecnorozmerny vektorovy priestor.
- $A \subseteq X$ - nezavisla mnozina vektorov.
- (i) $|A| < \aleph_0$
- (ii) A je LN $\Rightarrow A' \subseteq A$ je LN
- (iii) \emptyset je LN (trivialny dosledok (ii))
- (iv) $|A_1| < |A_2| \Rightarrow \exists x \in A_2 - A_1 : A_1 \cup \{x\}$ je LN

Matroid. Nech X je konečna množina, $N \subseteq P(X)$. Potom (X, N) je matroid, ak plati:

- N0) $\emptyset \in N$
- N1) $\forall A \in N : A' \subseteq A \Rightarrow A' \in N$ (dedicnost)
- N2) $\forall A, B \in N : |A| < |B| \Rightarrow \exists x \in B - A : A \cup x \in N$.

9.2 Specialne matroidy

Linearny matroid.

- $V = \{R_1, \dots, R_n\}$ vektory nad polom F .
- Nech $X = \{1, \dots, n\}$
- $\forall A : A \subseteq X \Rightarrow (A \in N \Leftrightarrow \{R_i, i \in A\} \text{ je LN})$
- Potom (X, N) je *linearny matroid*.

Grafovy matroid.

- $X = E(G)$
- A je acyklicka

9.3 Vlastnosti

Tvrdenie. Nech N_1, N_2 su maximalne matroidy vzhľadom na inklúziu. Potom $|N_1| = |N_2|$.

Baza matroidu. Bazou matroidu nazývame každú maximálnu nezávislú množinu vzhľadom na inklúziu.

Veta. Nech (X, S) je ľubovoľný systém (asi že $S \subseteq P(X)$). NPSE:

- (X, S) je matroid.
- S je neprázdny dedičný systém (t.j. N0, N1) spĺňajúci podmienku N2': $\forall A \subseteq X : \forall$ maximálne $B \subseteq A, B \in S$ majú rovnakú mohutnosť. Dokaz: keď nie, tak vieme doplniť.

9.4 Hodnotová funkcia

$r_u : P(X) \rightarrow \mathbb{N}, r_u(A) =$ najväčšia mohutnosť nezávislej množiny v A .

Veta. Nech $M = (X, N)$ je matroid, r je hodnotová funkcia. Potom platí:

-
-
-
-
-
-
-